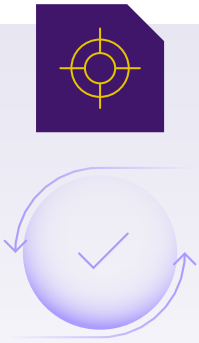
HUMAN

Cyberfraud Defense Checklist

Evaluation criteria to protect against threats from bots, humans, and AI agents

Standalone or bot-only security solutions fall short. Attackers orchestrate sophisticated attacks blending automation, AI-driven deception, and human-led fraud to exploit vulnerabilities across the entire customer journey. Defeating hybrid threats requires a comprehensive and adaptive defense strategy that protects every customer interaction, from account creation and authentication through transactions and beyond.

Use this checklist to evaluate cyberfraud solutions against seven essential criteria, ensuring comprehensive protection across the full customer journey. Validate vendor claims through independent research, including peer reviews and analyst evaluations like G2's seasonal grid and The Forrester Wave™: Bot Management Software, Q3 2024.

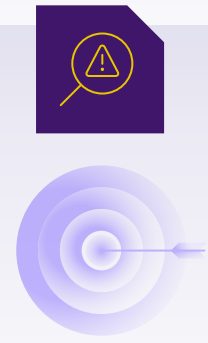


1. Threat Coverage

- ◯ Does the solution effectively defend against sophisticated, coordinated cyberfraud attacks spanning bots, human fraud, and AI-driven threats?
- ◯ Can the solution neutralize compromised credentials before they are used to commit fraud, block automated credential stuffing, and mitigate networks of compromised and fake accounts?
- ◯ Does it leverage multi-layered detection and customizable mitigation to protect every customer interaction, including pre-login site navigation, account login and signup, activity within accounts, and automated transactions?

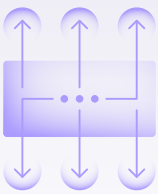
2. Impact on Performance and User Experience

- ◯ Does the solution maintain fast performance and add friction for bots without negatively impacting customer experience?
- ◯ How often are customers disrupted by challenges like CAPTCHAs or manual verifications?
- ◯ Can the solution prefilter malicious bots without requiring interaction from the end user?



3. Deployment and Management

- ◯ What resources and expertise are required for initial implementation and ongoing management?
- ◯ Does the solution have a mobile SDK? Does it support hybrid apps and APIs in addition to web?
- ◯ How responsive and effective is the vendor's customer support in addressing incidents or threats?



4. Fraud Detection and Mitigation

- Does the solution identify suspicious or illegitimate behavior within accounts and then quickly recover breached accounts earlier in the activity lifecycle, minimizing fraud incidents?
- Can users customize response actions, including out-of-the-box and API integrations with key systems (CIAM, SIEM, etc.)?
- Does a secondary detection engine analyze attack data post-decision to uncover hidden patterns, track changing threat behaviors, and automatically respond to specific adaptations?

5. Management of Good Bots and AI Agents

- Does the solution provide visibility and control over legitimate bots and AI agents interacting with your business?
- Can you customize policies and responses to manage trusted automation effectively?
- Does the solution allow the monetization of traffic from AI crawlers and scrapers on a pay-per-crawl basis?

6. Reporting and Investigation

- Does the solution offer dashboards tailored to fraud, security, and business stakeholders?
- Does the solution isolate automated traffic into distinct threats, enabling users to pinpoint distinct bot actions, characteristics, and behaviors over time?
- Does the solution identify and group networks of compromised and fake accounts being used for fraud?

7. Platform capabilities

- Does the vendor provide complementary cybersecurity solutions to address adjacent threats, such as client-side attacks ad fraud, or malvertising?
- Is there a dedicated threat intelligence team actively researching emerging cyberfraud tactics?
- Does the vendor have a demonstrated track record of innovation and responsiveness to evolving cyberfraud challenges?

HUMAN

About HUMAN

HUMAN is a leading cybersecurity company committed to protecting the integrity of the digital world. We verify that digital interactions, transactions, and connections are authentic, secure, and human. HUMAN verifies 20 trillion digital interactions weekly, providing unparalleled telemetry data to enable rapid, effective responses to the most sophisticated threats. Recognized by our customers as a leader in the G2 Grid and Forrester Wave, HUMAN continues to set the standard in cybersecurity. For more information, visit www.humansecurity.com.